UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/728,488	11/30/2000	Sunil K. Srivastava	50325-0108 (1590)	4277

29989 7590 09/28/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/728,488	SRIVASTAVA, SUNIL K.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11/30/00* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date See attached.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the communications filed on 13 June 2005.

2. Claims 1-58 are pending in the application.

3. Claims 1-58 have been rejected.

Specification

4. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract exceeds the 150-word limit.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 2, 4-6, 9-32, 34, 35 and 38-58 are rejected under 35 U.S.C. 102(b) as being anticipated by Dondeti et al U.S. Patent No. 6,240,188 B1.

As to claim 1, Dondeti et al discloses a method of establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, comprising the steps of:

receiving information defining a plurality of multicast proxy service nodes that are distributed across a local area network that is coupled to the wide area network and for controlling when any of the member nodes join or leave the multicast group, wherein the multicast proxy service nodes are logically represented by a first binary tree [column 3 line 58 to column 4 line 21];

creating and storing a second binary tree for representing the member nodes, wherein each of the member nodes is represented by a leaf node of the second binary tree, that is stored in a domain of a directory service that is distributed across the wide area network, and wherein each of the member nodes is capable of establishing multicast communication and serving as a key distribution center [column 3 line 58 to column 4 line 21];

creating and storing a group session key associated with the multicast group and a private key associated with each node in a group using secure key exchange [column 4 line 22 to column 5 line 10];

when one of the member nodes joins the multicast group, determining a new group session key by replicating a branch of the second binary tree.

As to claim 2, Dondeti et al discloses that each of the member nodes is associated with one of the multicast proxy service nodes, wherein each of the multicast proxy service nodes acts as one of a plurality of replicated group controllers, further comprising the steps of:

joining one of the group controllers to the plurality of replicated group controllers in the local area network [column 6 line 22 to column 8 line 42];

establishing, by one of the group controllers, a secure communication channel between one of the group controllers and another of the group controllers using a key exchange protocol [column 6 line 22 to column 8 line 42];

receiving a request to add or delete the specified member node of the multicast group from a load balancer that is coupled to the plurality of group controllers [column 6 line 22 to column 8 line 42];

creating and storing a new group session key for each member node in each branch of the tree that is affected by adding or deleting the specified member node from the group [column 6 line 22 to column 8 line 42];

distributing the new group session key from one of the group controllers to the affected member nodes [column 6 line 22 to column 8 line 42].

As to claim 4, Dondeti et al discloses a method wherein distributing a group session key further comprises:

determining whether the multicast group has a node that is leaving the multicast group c;

determining which of the intermediate nodes are affected by the leaving node [column 8 line 44 to column 10 line 39];

updating only keys associated with the affected intermediate nodes [column 8 line 44 to column 10 line 39];

generating a new group session key [column 8 line 44 to column 10 line 39]; and

sending the new group session key to the leaf nodes [column 8 line 44 to column 10 line 39].

As to claim 5, Dondeti et al discloses a method wherein updating keys comprises:

generating a new key of a parent node of the leaving node [column 8 line 44 to column 10 line 39]; and

encrypting the new key of the parent node with an existing key of the member node that is adjacent to the parent node [column 8 line 44 to column 10 line 39].

As to claim 6, Dondeti et al discloses a method wherein distributing a group session key further comprises:

receiving a request message from one of the plurality of member nodes to join the multicast group [column 6 line 22 to column 8 line 42];

determining which of the intermediate nodes are affected by the joining node [column 6 line 22 to column 8 line 42];

updating only keys associated with the affected intermediate nodes [column 6 line 22 to column 8 line 42];

generating a new group session key and a private key for the joining node; and

sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node [column 6 line 22 to column 8 line 42].

As to claim 9, Dondeti et al discloses a method wherein establishing a secure communication channel comprises:

receiving a public key value that is broadcast by the joining node [column 6 line 22 to column 8 line 42] ;

sending a collective public key value from the nodes to the joining node[column 6 line 22 to column 8 line 42];

computing a shared secret key [column 6 line 22 to column 8 line 42];

creating and storing a group shared secret key by exchanging private key values [column 6 line 22 to column 8 line 42].

As to claim 10, Dondeti et al discloses that determining a new group session key comprises computing a group shared secret key at a first member node for use in a public key process and using less than n * (n-1) messages, where "n" is a number of member nodes in a broadcast or multicast group, by the steps of:

generating an intermediate shared secret key by issuing communications to a second member node [column 6 line 43 to column 7 line 13];

sending a first private value associated with the first member node to the second member node, and receiving from the second member node a second private value associated with the second member node using the intermediate shared secret key [column 6 line 43 to column 7 line 13];

generating and communicating a collective public key that is based upon the first private value and the second private value to a third member node of the network [column 6 line 43 to column 7 line 13];

receiving an individual public key from the third member node [column 6 line 43 to column 7 line 13]; and

computing and storing the group shared secret key based upon the individual public key [column 6 line 43 to column 7 line 13].

As to claim 11, Dondeti et al discloses a method further comprising:

joining the first member node to an initial multicast group in response to generating the intermediate shared secret key [column 6 line 22 to column 8 line 42]; and

joining a second member node to a new multicast group that subsumes the initial multicast group after receiving the individual public key [column 6 line 22 to column 8 line 42].

As to claim 12, Dondeti et al discloses that the step of communicating the collective public key further comprises determining whether the first member node or the second member node transfers the collective public key based upon an order of entry of such member nodes into a multicast group [column 6 line 43 to column 7 line 13].

As to claim 13, Dondeti et al discloses sending the first private value and receiving the second private value further comprises computing the first private value as a random integer and receiving a second random integer as the second private value [column 6 line 43 to column 7 line 13].

As to claim 14, Dondeti et al suggests the step of establishing a cryptographic communication session between the first member node and the second member node, whereby secure communications are established between the first member node and the second member node using public key exchange and only approximately 2n + 2(n-1) total messages, wherein n represents a number of the member nodes [column 4, lines 49-65].

As to claim 15, Dondeti et al suggests that generating the shared secret key value comprises computing and storing the shared secret key value "k" at the first member node according to the relation

$$k = C^{ab} \bmod (q) = p^{abc} \bmod (q)$$ [column 4, lines 49-65]

wherein C, a, b, c, q, and p are values stored in a memory, and wherein C is the individual public key, a is the private value of the first member node, b is the private value of the second member node, c is a third private value of the third member node, p is a base value, and q is a prime number value [column 4, lines 49-65].

As to claim 16, Dondeti et al discloses that determining a new group session key comprises computing a group shared secret key, each of the member nodes having a private key value associated therewith, by the steps of:

communicating a first public key value of the first member node to a second member node [column 8, lines 16-42];

creating and storing an initial shared secret key for the first member node and second member node based on a first private key value and a second public key value that is received from the second member node [column 8, lines 16-42];

creating and storing information at the first member node that associates the first member node with a first network communication entity by generating a collective public key value that is shared by the first member node and a second member node and based on the first private key value and a second private key value that is derived by the first member node from the second public key valu [column 8, lines 16-42]e;

receiving a third public key value from a third member node that seeks to join the first network communication entity [column 8, lines 16-42];

creating and storing a shared secret key value based on the collective public key value and the third public key value [column 8, lines 16-42];

joining the first member node to a second network communication entity that includes the first network communication entity and the third member node and that uses secure communication with messages that are encrypted using the shared secret key value [column 8, lines 16-42].

As to claim 17, Dondeti et al discloses that joining the first member node to a second network communication entity includes the step of communicating the first private key value to the second member node and to the third member node using messages encrypted using the shared secret key value [column 8, lines 16-42].

As to claim 18, Dondeti et al discloses that creating and storing a shared secret key value further comprises creating and storing the shared secret key based upon how many times each member node of the second network communication entity has participated in formation of any

such entity and based upon each private number of each member node in the second network communication entity [column 7, lines 43-63].

As to claim 19, Dondeti et al discloses the step of creating and storing a subsequent shared secret key for use by the first network communication entity and the third node to enable the third node to independently compute the group shared secret key [column 7, lines 43-63].

As to claim 20, Dondeti et al suggests that creating and storing the subsequent shared secret key comprises creating and storing the subsequent shared secret key, k, according to the relation

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$ [column 4, lines 49-65]

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third member node, x = a number of times the first member node has participated in entity formation, y = a number of times the second member node has participated in entity formation, and z = a number of times the third member node has participated in entity formation [column 4, lines 49-65].

As to claim 21, Dondeti et al discloses that the step of joining the first member node to a second network communication entity further comprises:

creating and storing a collective public key based upon the first private key value, the second private key value, and the third private key value [column 7, lines 43-63];

communicating a collective public key of the second network communication entity to the third member node [column 7, lines 43-63].

As to claim 22, Dondeti et al discloses that the step of joining the first member node to a second network communication entity further comprises determining which one of the member nodes of the first network communication entity is designated to transfer the collective public key based upon order of entry into the formed entity.

As to claim 23, Dondeti et al suggests that creating and storing an initial shared secret key for the first member node and second member node comprises creating and storing an initial shared public key "AB" according to the relation

$AB = k_{ab}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$ [column 4, lines 49-65]

wherein k = the initial shared secret key value, a = the first private key value, b = the second private key value, p is a base value, and q is a randomly generated prime number value [column 4, lines 49-65].

As to claim 24, Dondeti et al discloses a method further comprising the steps of:

authenticating a first event service node with a subset of the event service nodes that are affected by an addition of the first event service node to the multicast group, based on key information stored in a directory [column 10 line 61 to column 11 line 36];

receiving a plurality of private keys from the subset of nodes [column 10 line 61 to column 11 line 36];

generating a new private key for the first event service node [column 10 line 61 to column 11 line 36];

communicating the plurality of private keys and the new private key to the first event service node [column 10 line 61 to column 11 line 36];

communicating a message to the subset of nodes that causes the subset of nodes to update their private keys [column 10 line 61 to column 11 line 36].

As to claims 25 and 26, Dondeti et al discloses that authenticating the plurality of event service nodes based on information stored in a directory includes authenticating the plurality of event service nodes based on a directory that comprises a directory system agent (DSA) for communicating with one or more of the event service nodes and a replication service agent (RSA) for replicating attribute information of the one or more event service nodes [column 10 line 61 to column 11 line 36]. Dondeti et al discloses that the attribute information comprises a group session key and the private keys [column 10 line 61 to column 11 line 36].

As to claim 27, Dondeti et al discloses that generating private keys comprises generating private keys for each of the intermediate nodes and leaf nodes, the private keys providing unique identification within the tree structure, and wherein each private key is N bits in length, wherein each bit corresponds to one of the private keys, and N is an integer [column 5 line 36 to column 6 line 4].

As to claim 28, Dondeti et al discloses distributing a group session key to all nodes by creating and storing the group session key using a first event service node of one domain of the directory [column 5 line 36 to column 6 line 4]. Dondeti et al discloses replicating the directory [column 10 line 61 to column 11 line 36]. Dondeti et al discloses obtaining the group session key from a local event service node that is a replica of the first event service node [column 10 line 61 to column 11 line 36].

As to claim 29, Dondeti et al discloses that generating private keys comprises generating private keys for each of the intermediate nodes and leaf nodes [column 3 line 48 to column 4 line

65]. Dondeti et al discloses the private keys providing unique identification within the tree structure [column 3 line 48 to column 4 line 65]. Dondeti et al discloses that each private key is N bits in length [column 3 line 48 to column 4 line 65]. Dondeti et al discloses that each bit corresponds to one of the private keys, and N is an integer [column 3 line 48 to column 4 line 65]. Dondeti et al discloses that the most significant bits of the N bits correspond to nodes logically near the root node in the tree structure [column 3 line 48 to column 4 line 65].

As to claim 30, Dondeti et al discloses selectively updating a group session key for use in encrypting communications among all nodes in the multicast group and selectively updating the private keys [column 3 line 48 to column 4 line 65].

As to claim 31, Dondeti et al discloses a method further comprising selectively updating the group session key and the private keys by:

detecting whether a network node associated with one of the leaf nodes is leaving the secure multicast or broadcast group [column 8 line 44 to column 9 line 19];

determining tree nodes along a tree path corresponding to the leaving leaf node are affected in response to the detecting step [column 8 line 44 to column 9 line 19];

updating the private keys of the affected intermediate nodes [column 8 line 44 to column 9 line 19];

generating a new group session key [column 8 line 44 to column 9 line 19];

modifying the attribute information based upon the updated private keys and the new group session key [column 8 line 44 to column 9 line 19]; and

generating instructions that distribute the modified attribute information using directory replication [column 8 line 44 to column 9 line 19].

As to claim 32, Dondeti et al discloses that the step of generating the new group session key is performed by one of the affected intermediate nodes that is the parent node of the leaving leaf node [column 8 line 44 to column 9 line 19]. Dondeti et al discloses the one affected intermediate node selectively sending the new group session key to all ancestral nodes along the tree path [column 8 line 44 to column 9 line 19].

As to claim 34, Dondeti et al discloses a method further comprising selectively updating a group session key and the private keys, wherein the step of selectively updating comprises:

receiving a request message from a new network node to join the secure multicast group [column 6 line 22 to column 8 line 13];

determining which of the intermediate nodes along a tree path corresponding to the new leaf node are affected in response to the receiving step [column 6 line 22 to column 8 line 13];

updating the private keys of the affected intermediate nodes [column 6 line 22 to column 8 line 13];

generating a new group session key and a private key of the new leaf node [column 6 line 22 to column 8 line 13];

modifying the attribute information based upon the updated private keys, the new group session key, and the private key of the new leaf node [column 6 line 22 to column 8 line 13]; and

distributing the modified attribute information using directory replication [column 6 line 22 to column 8 line 13].

As to claim 35, Dondeti et al discloses that one of the affected intermediate nodes that is the parent node of the new leaf node requests permission from the root node to generate the new session key [column 6 line 22 to column 8 line 13].

As to claim 38, Dondeti et al discloses a method further comprising the steps of:

creating and storing a group session key associated with the multicast group in the directory service [column 3 line 30 to column 4 line 65];

authenticating a first multicast proxy service node with a subset of the multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the multicast group, based on the group session key stored in the directory [column 3 line 30 to column 4 line 65];

receiving a plurality of private keys from the subset of nodes [column 3 line 30 to column 4 line 65];

receiving a new group session key for the multicast group, for use after addition of the first multicast proxy service node, from a local multicast proxy service node that has received the group session key through periodic replication of the directory [column 3 line 30 to column 4 line 65];

communicating the new group session key private key to the first multicast proxy service node [column 3 line 30 to column 4 line 65];

communicating a message to the subset of nodes that causes the subset of nodes to update their private keys [column 3 line 30 to column 4 line 65].

As to claim 39, Dondeti et al discloses that authenticating the plurality of multicast proxy service nodes includes authenticating the plurality of multicast proxy service nodes using a directory system agent (DSA) that communicates with one or more of the multicast proxy service nodes and a replication service agent (RSA) that replicates attribute information of the one or more multicast proxy service nodes [column 10 line 61 to column 11 line 36].

As to claim 40, Dondeti et al discloses that receiving a new group session key includes receiving the new group session key from a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes and a replication service agent (RSA) for replicating key information of the one or more multicast proxy service nodes [column 10 line 61 to column 11 line 36].

As to claim 41, Dondeti et al discloses the step of signaling the replication service agent to carry out replication by storing an updated group session key in a local node of the directory [column 3 line 30 to column 4 line 65].

As to claims 42 and 43, Dondeti et al discloses distributing a group session key to all nodes by creating and storing the group session key using a first multicast proxy service node of one domain of the directory [column 3 line 30 to column 4 line 65]. Dondeti et al discloses replicating the directory [column 10 line 61 to column 11 line 36]. Dondeti et al discloses

obtaining the group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node [column 10 line 61 to column 11 line 36].

As to claim 44, Dondeti et al discloses a method wherein determining a new group session key comprises the steps of:

receiving information indicating that a specified node is joining the multicast group [column 6 line 22 to column 8 line 13];

updating all affected keys of a subset of member nodes in a branch of the second binary tree that contains the specified joining node [column 6 line 22 to column 8 line 13];

receiving a new group session key for the multicast group, for use after addition of the specified joining node, and a new private key for the specified joining node, from one of the member nodes that is local to the specified joining node [column 6 line 22 to column 8 line 13];

communicating a message to the subset of member nodes that causes the subset of member nodes to update their private keys [column 6 line 22 to column 8 line 13].

As to claim 45, Dondeti et al discloses a method further comprising the steps of:

associating a plurality of intermediate nodes of the binary tree with a plurality of multicast service agents [column 11, lines 39-57];

establishing a secure back channel group among the multicast service agents [column 11, lines 39-57];

updating the group session key to all the multicast service agents by securely communicating the group session key using the secure back channel [column 11, lines 39-57].

As to claim 46, Dondeti et al discloses a method further comprising the steps of:

associating a plurality of intermediate nodes of the binary tree with a plurality of multicast service agents, wherein the multicast service agents are distributed across a wide area network [column 11, lines 39-57];

establishing a secure back channel group among the multicast service agents [column 11, lines 39-57];

updating the group session key to all the multicast service agents across the wide area network by securely communicating the group session key using the secure back channel [column 11, lines 39-57].

As to claim 47, Dondeti et al discloses a method further comprising the steps of:

associating a plurality of intermediate nodes of the binary tree with a plurality of multicast service agents [column 10 line 29 to column 11 line 14];

establishing a secure back channel group among the multicast service agents [column 11, lines 39-57];

updating the group session key to all the multicast service agents by securely communicating the group session key using the secure back channel [column 10 line 29 to column 11 line 14];

at each intermediate node, updating the group session key of only those leaf nodes that are child nodes of the intermediate node [column 10 line 29 to column 11 line 14].

As to claim 48, Dondeti et al discloses a method further comprising the steps of:

receiving a request for the group session key from a publisher node that is located in a different domain from the group controller node [column 3, lines 30-63];

determining an identifier of the publisher node using a local directory service agent [column 3, lines 30-63];

establishing a secure communication channel among the group controller node and a directory service agent in the different domain. [column 3, lines 30-63]

As to claim 49, Dondeti et al discloses the method further comprising selectively updating the group session key and the private keys by:

detecting whether a network node is leaving the secure multicast or broadcast group [column 8 line 44 to column 9 line 19];

determining nodes that are affected in response to the detecting step [column 8 line 44 to column 9 line 19];

updating the private keys of the affected intermediate nodes [column 8 line 44 to column 9 line 19];

generating a new group session key [column 8 line 44 to column 9 line 19];

modifying the attribute information based upon the updated private keys and the new group session key [column 8 line 44 to column 9 line 19]; and

requesting to distribute the modified attribute information using directory replication [column 8 line 44 to column 9 line 19].

As to claim 50, Dondeti et al discloses a method further comprising selectively updating a group session key and the private keys, wherein the step of selectively updating comprises:

receiving a request message from a new network node to join the secure multicast group [column 6 line 22 to column 8 line 13];

determining which of the intermediate nodes are affected in response to the receiving step [column 6 line 22 to column 8 line 13];

updating the private keys of the affected intermediate nodes [column 6 line 22 to column 8 line 13];

generating a new group session key and a private key of the new node [column 6 line 22 to column 8 line 13];

modifying the attribute information based upon the updated private keys, the new group session key, and the private key of the new node [column 6 line 22 to column 8 line 13]; and

distributing the modified attribute information to all the affected nodes [column 6 line 22 to column 8 line 13].

As to claim 51, Dondeti et al discloses a method further comprising managing removal of a first node from the secure multicast group that comprises the first node and a plurality of the multicast proxy service nodes, by the steps of:

creating and storing a group session key associated with the multicast group and a private key associated with each node in a directory [column 3 line 30 to column 4 line 65];

receiving information indicating that the first node is leaving the multicast group [column 3 line 30 to column 4 line 65];

updating all affected keys of a subset of nodes in a branch of the binary tree that contains the leaving node [column 3 line 30 to column 4 line 65];

receiving a new group session key for the multicast group, for use after removal of the first node, and a new private key for the first node, from a local group controller node [column 3 line 30 to column 4 line 65];

communicating a message to the subset of nodes that causes the subset of nodes to update their private keys [column 3 line 30 to column 4 line 65].

As to claim 52, Dondeti et al discloses a method further comprising the steps of:

associating a plurality of intermediate nodes of the binary tree with a plurality of multicast service agents [column 10 line 29 to column 11 line 14];

establishing a secure back channel group among the multicast service agents [column 10 line 29 to column 11 line 14];

changing a private key associated with one of the intermediate nodes, in response to receiving information indicating that the first node is leaving the multicast group [column 10 line 29 to column 11 line 14];

updating a group controller of the binary tree with the changed private key by sending the changed private key by securely communicating using the secure back channel [column 10 line 29 to column 11 line 14].

As to claim 53, Dondeti et al discloses a method further comprising the steps of:

associating a plurality of intermediate nodes of the binary tree, including the first node, with a plurality of multicast service agents [column 10 line 29 to column 11 line 14];

establishing a secure back channel group among the multicast service agents [column 10 line 29 to column 11 line 14];

changing a plurality of private keys associated with all nodes that are child nodes of the first node, in response to receiving information indicating that the first node is leaving the multicast group [column 10 line 29 to column 11 line 14];

updating a group controller of the binary tree with the changed private keys by decrypting the group session key from the group controller and then encrypting the group session key with the changed private keys [column 10 line 29 to column 11 line 14].

As to claim 54, Dondeti et al discloses a method further comprising the steps of:

associating a plurality of intermediate nodes of the binary tree with a plurality of multicast service agents [column 5 line 53 to column 6 line 4];

establishing a secure back channel group among the multicast service agents [column 5 line 53 to column 6 line 4];

updating the group session key to all the multicast service agents by securely communicating the group session key using the secure back channel [column 5 line 53 to column 6 line 4];

at each intermediate node, updating the group session key of only those leaf nodes that are child nodes of the intermediate node [column 5 line 53 to column 6 line 4].

As to claim 55, Dondeti et al discloses a method further comprising the steps of:

receiving a request for the group session key from a publisher node that is located in a different domain from the group controller node [column 4, lines 29-63];

determining an identifier of the publisher node using a local directory service agent [column 4, lines 29-63];

establishing a secure communication channel among the group controller node and a directory service agent in the different domain [column 4, lines 29-63].

As to claim 56, Dondeti et al discloses a method further comprising distributing a group session key to all nodes by creating and storing the group session key using a first multicast proxy service node of one domain of the directory; replicating the directory; and obtaining the group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node [column 4, lines 29-63].

As to claim 57, Dondeti et al discloses a communication system for establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, the communication system comprising:

a group controller that creates and manages secure multicast communication among the other multicast proxy service nodes, having a private key [column 3 line 58 to column 4 line 21];

a computer-readable medium comprising one or more instructions which, when executed by one or more processors, cause the one or more processors to carry out the steps of:

establishing a plurality of multicast proxy service nodes that are distributed across a local area network that is coupled to the wide area network and for controlling when any of the member nodes join or leave the multicast group, wherein the multicast proxy service nodes are logically represented by a first binary tree [column 3 line 58 to column 4 line 21];

creating and storing a second binary tree for representing the member nodes, wherein each of the member nodes is represented by a leaf node of the second binary tree, that is stored in a domain of a directory service that is distributed across the wide area network, and wherein each of the member nodes is capable of establishing multicast communication and serving as a key distribution center [column 3 line 58 to column 4 line 21];

creating and storing a group session key associated with the multicast group and a private key associated with each node in a group using secure key exchange [column 4 line 22 to column 5 line 10];

when one of the member nodes joins the multicast group, determining a new group session key by replicating a branch of the second binary tree [column 4 line 22 to column 5 line 10].

As to claim 58, Dondeti et al discloses a computer-readable medium carrying one or more sequences of instructions for establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

establishing a plurality of multicast proxy service nodes that are distributed across a local area network that is coupled to the wide area network and for controlling when any of the member nodes join or leave the multicast group, wherein the multicast proxy service nodes are logically represented by a first binary tree [column 3 line 58 to column 4 line 21];

creating and storing a second binary tree for representing the member nodes, wherein each of the member nodes is represented by a leaf node of the second binary tree, that is stored in a domain of a directory service that is distributed across the wide area network, and wherein each of the member nodes is capable of establishing multicast communication and serving as a key distribution center [column 3 line 58 to column 4 line 21];

creating and storing a group session key associated with the multicast group and a private key associated with each node in a group using secure key exchange [column 4 line 22 to column 5 line 10];

when one of the member nodes joins the multicast group, determining a new group session key by replicating a branch of the second binary tree [column 4 line 22 to column 5 line 10].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dondeti et al U.S. Patent No. 6,240,188 B1 as applied to claim 1 above, and further in view of Hosein U.S. Patent No. 6,570,847 B1.

As to claim 3, Dondeti et al does not teach that distributing a group session key further comprises:

receiving a token value at the group controller to designate the group controller as having permission to selectively generate the new group session key and to generate node keys associated with the affected intermediate nodes and the leaf nodes; and

creating and storing the new group session key only when the group controller has the token value.

Hosein teaches receiving a token value at the group controller to designate the group controller as having permission to selectively generate the new group session key and to generate node keys associated with the affected intermediate nodes and the leaf nodes [column 2 line 54 to column 3 line 42]. Hosein teaches creating and storing the new group session key only when the group controller has the token value [column 2 line 54 to column 3 line 42].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dondeti et al so that there would have been a token value received at the group controller to designate the group controller as having permission to selectively generate the new group session key and to generate node keys associated with the affected intermediate nodes and the leaf nodes. The new group session key would have been created and stored only when the group controller has the token value.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dondeti et al by the teaching of Hosein because the token values provide regulation and control over network traffic to bring stability and efficiency to the network infrastructure [column 1, lines 14-26].

7. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dondeti et al U.S. Patent No. 6,240,188 B1 as applied to claim 1 above, and further in view of Ladwig et al U.S. Patent No. 6,247,014 B1.

As to claim 7, Dondeti et al does not teach that updating keys comprises performing a one way hash function on the keys associated with the affected intermediate nodes.

Ladwig et al teaches that updating keys comprises performing a one way hash function on the keys associated with the affected intermediate nodes [column 5 line 10 to column 6 line 11].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dondeti et al so that keys would have been updated by performing a one way function on the keys associated with the affected nodes.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dondeti et al by the teaching of Ladwig et al because hashing keys provides a method to verify that the keys have not been modified or changed during transmission.

8. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dondeti et al U.S. Patent No. 6,240,188 B1 as applied to claim 1 above, and further in view of Newton's Telecom Dictionary (hereinafter Newton).

As to claim 8, Dondeti et al teaches establishing a secure communication channel comprises exchanging a public key of the group controller with all other group controllers in the plurality of replicated group controllers.

Dondeti et al does not teach that the key exchange is based upon optimized broadcast Diffie-Hellman protocol.

Newton teaches key exchange using the Diffie-Hellman protocol and its benefits [page 228].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dondeti et al so that a secure communication

channel would have been established. A public key would have been exchanged with all other group controllers in the plurality of replicated group controllers using a key exchange based upon optimized broadcast Diffie-Hellman protocol.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dondeti et al by the teaching of Newton because the Diffie-Hellman key exchange protocol provides a significant cost advantage by eliminating the need for a courier service. In addition, security can considerably enhanced by permitting more frequent key changes and eliminating the need for any individual to have access to the key's actual value [page 228].

9. Claims 33 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dondeti et al U.S. Patent No. 6,240,188 B1 as applied to claim 1 above, and further in view of Ladwig et al U.S. Patent No. 6,247,014 B1.

As to claims 33 and 36, Dondeti et al does not teach that the step of updating the private keys of the intermediate nodes comprises performing a one way hash function on the private keys in response to receiving a corresponding instruction from the root node.

Ladwig et al teaches performing a one way hash function on the private keys in response to receiving a corresponding instruction from the root node [column 5 line 10 to column 6 line 11].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dondeti et al so that the step of updating the private keys of the intermediate nodes would have comprised performing a one way hash

function on the private keys in response to receiving a corresponding instruction from the root node.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dondeti et al by the teaching of Ladwig et al because hashing keys provides a method to verify that the keys have not been modified or changed during transmission.

10. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dondeti et al U.S. Patent No. 6,240,188 B1 as applied to claim 1 above, and further in view of Friedman et al U.S. Patent No. 6,240,513 B1.

As to claim 37, Dondeti et al does not teach that generating the private keys comprises generating the private keys based upon an Internet Protocol (IP) address and time values.

Friedman et al teaches generating the private keys based upon an Internet Protocol (IP) address and time values [column 10, lines 27-49].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dondeti et al so that the private keys were generated based upon an IP address and a time-stamp.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dondeti et al by the teaching of Friedman et al because it generates static keys. The static key are permanent keys unique to each device [column 5, lines 38-46.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Primary Examiner
AU2131
9/23/05

Aravind K Moorthy AM
September 21, 2005